UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,970	11/17/2003	Sundeep M. Bajikar	42.P18073	5365

8791 7590 01/11/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
SHAN, APRIL YING	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
01/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/715,970	BAJIKAR, SUNDEEP M.	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A Request for Continued Examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 24 October 2007 has been entered.

2. Claims 1-3, 13, 15, 18 and 20 have been amended. No new claims have been added. Claims 1- 24 are currently pending in the present application.

3. Applicant's amendments and argument have been fully considered, but are moot in view of new ground rejection as set forth below. It is noted that Applicant's arguments are directed towards limitations newly added via amendments.

4. Any objections/rejections not repeated below for record are withdrawn due to Applicant's amendment.

Information Disclosure Statement

5. The information disclosure statement filed 25 April 2005 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in

the English language. It has been placed in the application file, but the information referred to therein has not been considered: DE 10004164A1.

6. The information disclosure statement filed 10 November 2004 contains publications that have not been considered because they are not analogous art or within the same field of endeavor: U.S. Patent No. 5,582,717 (water cooler), U.S. Patent No. 5,720,609 (Catalytic Method for petrol), U.S. Patent No. 5,721,222 (Heterocyclic Ketons – organic biology), U.S. Patent No. 5,796,835 (Sound system enhancement – analog circuit), U.S. Patent No. 6,158,546 (Car muffler).

Drawings

7. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. In the current fig. 2, step 206 appears to the examiner that encryption key might be an unencrypted data as recited in the claims 1 and 13. The Applicant is respectfully requested to confirm in the response to the current office action that unencrypted data = encryption key. Otherwise, "unencrypted data" in the amended claims 1, 2 and 13-14 must be shown or the feature(s) canceled from the (s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet,

and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

8. Claim 9 is objected to because of the following informalities:

a. For claim 9, "exchanging a encryption key" should be "exchanging an encryption key";

Please check the claims 1-24 and correct any informality the Applicant is aware of. Appropriate corrections are required.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 1-24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to

which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per **claims 1-2 and 13-14**, "exchanging unencrypted data" and "wherein the exchanging of data include... exchanging data encrypted with the encryption key" are being recited. In fig. 2 of the original disclosure, it appears to the examiner that in step 206, encryption key is an unencrypted data transmitted to protected memory and in step 212, encryption data is transmitted to unprotected memory. However, in the independent claims, exchanging unencrypted data is being recited and in the dependent claims wherein the exchanging of data appears to the examiner is the exchanging of unencrypted data further includes exchanging of encrypted data, these two limitations are contradicted with each other and the original disclosure and therefore, they are not enabling.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> **The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.**

12. Claims 1-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claims 1 and 13**, "exchanging unencrypted data" is being recited. And in claims 2 and 14, "wherein the exchanging of data include... exchanging data encrypted

with the encryption key" is being recited. However, in the independent claims 1 and 13, "exchanging unencrypted data" is being recited. It appears to the examiner that exchanging data encrypted with the encryption key is not further limit the independent claims and contradicted with the independent claims and dependent claims 2 and 14 appear to be broader than the independent claims 1 and 13.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

15. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gehrmann et al. (U.S. Pub. No. 2004/0176071) in view of WO 01/75595 A2 (hereinafter '75595)

As per **claims 1 and 13**, Gehrmann et al. discloses a method/system, comprising: exchanging unencrypted data (e.g. par. [0075] – [0077], steps 505 and 506 in fig. 5/steps 605 and 506 in fig. 6) between a SIM device ("subscription module" – e.g. paragraphs [0065] and [0072]. Please note in paragraph [0017], Gehrmann et al. expressly define the term subscription module comprises modules which may be removably inserted into a communications terminal, such as a SIM card. Therefore, subscription module corresponds to Applicant's SIM device. Please further note in par. [0066], "In order to encrypt the messages the RAA client and the subscription module use the new shared secret exchanged in step 505" and in par. [0065], Diffie-Hellman protocol is disclosed. The Diffie-Hellman protocol exchange keys in the clear and the keys are not encrypted and therefore, the key exchanged in Gehramann et al. is an encryption key and unencrypted) and an application executed in a trusted platform (e.g. paragraphs [0065]-[d] and [0084] – [0085]. Please note client communications terminal corresponds to Applicant's an application executed in a trusted platform), via a trusted path within a computer system (e.g. par. [0065] and [0084]), the trusted path being a path through a trusted port ("...The subscription module further comprises an input/output **interface** 206 for communicating with the device it is inserted in..." – e.g. par. [0060], "...the communication over the **interface** provided by the subscription module, is **protected**" – e.g. par. [0022], "...a wireless **interface** and the **subscription module** may be implemented as **one physically inseparable entity**" – e.g. par. [0032], "...Therefore, it is an advantage of the invention that **it secures all interfaces** when providing remote access..." – e.g. par. [0061], [0037] and fig. 2. Please note protected

interface and secures all interfaces correspond to Applicant's a trusted port) of a chipset (e.g. par . [0036], [0038], [0040], [0049] and [0064]-[0065]. Please note subscription module, processing means, circuit and communication means correspond to Applicant's chipset) wherein the unencrypted data to be exchanged is secured from unauthorized access ("Preferably, this key exchange may be a part of the authentication procedure. Alternatively, the key exchange is performed after successful authentication. The authentication and key exchange can be done in several different ways using well known state of art solutions... Diffie-Hellman..." – e.g. par. [0065]).

Gehrmann et al. does not expressly disclosed wherein the trusted port is mapped to a protected section of memory that is inaccessible to direct memory access. However, this well known feature is disclosed in '75595 (e.g. abstract, pages 5-8 and 16). It would have been obvious to a person with ordinary skill in the art to combine the well known feature of '75595 with Gehrmann et al. to provide security in a computer system or platform.

As per **claims 2 and 14**, Gehrmann et al. – '75597 discloses a method/system as applied above in claims 1 and 13. Gehrmann et al. – '75597 further discloses wherein the exchanging of data include: exchanging an encryption key via the trusted path within the computer system (e.g. Gehrmann et al. , paragraphs [0065] and [0084]. Please also see the rationale of rejecting claim 1 above); and exchanging data encrypted with the encryption key (e.g. paragraphs [0066] and [0085]), via an untrusted

path within the computer system (Gehrmann et al., e.g. paragraph [0022], [0061] and fig. 3), the untrusted path being a path through an untrusted port of the chipset , wherein the untrusted port is mapped to an unprotected section of memory what is accessible to direct memory access ('75595, e.g. abstract, pages 5-8 and 16)

As per **claims 3 and 15**, Gehrmann et al. - – '75597 discloses a method/system as applied above in claims 2 and 14. Gehrmann et al. further discloses wherein the exchanging the encryption key includes the application transmitting the encryption key to a protected section of memory within the computer system (e.g. paragraph [0065]); and a SIM device accessing the encryption key from the protected section of memory (e.g. paragraph [0065]).

As per **claims 4 and 16**, Gehrmann et al. – '75597 discloses a method/system as applied above in claims 2 and 14. Gehrmann et al. further discloses wherein the exchanging the encryption key includes the application accessing the encryption key from the SIM device (e.g. paragraph [0065]), the application accessing the encryption key via the trusted port of the chipset (e.g. paragraphs [0064]-[0065]).

As per **claims 5 and 17**, Gehrmann et al. – '75597 discloses a method/system as applied above in claims 2 and 14. Gehrmann et al. further discloses wherein the exchanging the encryption key includes exchanging multiple encryption keys ("..multiple keys...." – e.g. paragraph [0060], "a number of secret key codes K-1 through K-N...the keys may be 128 bit symmetric keys" – e.g. paragraph [0064]), and the exchanging data

includes exchanging separate units of data ("...PIN codes, authorization codes, identifiers, account numbers, all messages..." – e.g. paragraph [0066]. Please note all messages such as PIN codes, account numbers corresponds to Applicant's separate units of data).

Gehrmann et al. discloses in the paragraph [0062], "the shared secret may be a secret key which is created when needed and which is valid for a specific time period, for one session, or the like, i.e. it is a temporary shared secret" and in par. [0076], "The subscription module asks...for the public key(s)..." Therefore, multiple encryption keys can be multiple encryption session keys for encrypting multiple sessions/units of data.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to encrypt each unit of data separately with an encryption key selected from the multiple encryption keys.

As per **claims 6-8, 12, 18-20 and 24**, Gehrmann et al. – '75597 discloses a method/system as applied above in claims 2 and 14. Gehrmann et al. further discloses wherein the exchanging data includes a host controller transmitting data from the SIM device to an unprotected section of memory ("The interfaces 304 and 306 may be implemented as plug-in interfaces...such as USB or the like...as the interfaces 304 and/or 306 of the base module are open and, thus vulnerable for unauthorized access..." – e.g. paragraph [0061]. Please note to one with ordinary skill in the art, when using USB, there is a memory section to store USB data packets, which is

vulnerable for unauthorized access as disclosed by Gehrmann et al. Therefore, it met the claim limitation of unprotected memory section disclosed by the Applicant), wherein the exchanging data includes a driver transmitting data from the unprotected section of memory to the application (e.g. paragraph [0061]), wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver (e.g. paragraph [0061]) and further including: exchanging a new encryption key based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time ("...the shared secret may be a secret key which is created when needed and which is valid for a specific time period, for one session, or the like, i.e. it is a temporary shared secret" – e.g. paragraphs [0062]) and [0068]-[0071]) and exchange of a predetermined amount of data (e.g. paragraph [0062]).

As per **claims 9 and 21**, Gehrmann et al. – '75597 discloses a method/system as applied above in claims 2 and 14. Gehrmann et al. further discloses wherein the exchanging an encryption key includes the SIM device reading the encryption key from a protected section of memory via the trusted port of the chip set (e.g. paragraph [0064]-[0065]).

As per **claims 10 and 22**, Gehrmann et al. – '75597 discloses a method/system as applied above in claims 2 and 14. Gehrmann et al. further discloses including: the

application decrypting the encrypted data using the encryption key (e.g. paragraph [0066]).

As per **claims 11 and 23**, Gehrmann et al. – '75597 discloses a method as applied above in claims 2 and 14. Gehrmann et al. further discloses including prior to exchanging the encryption key, the application authenticating the SIM device (e.g. paragraph [0084] and step 604 in fig. 6).

Double Patenting

16. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

17. Claims 1, 2 and 13 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 2, 11, 15, 19 and 23 of copending Application No. 10/977,158 (U.S. Publication No. 2006/0075259). Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1, 2 and 13 encompass the same subject matter as claims 1, 2, 11, 15, 19 and 23 in the copending application.

Claim 1 recites a method comprising: exchanging (The term "exchanging" is interpreted as having the same meaning "transmitting..between" in the copending application) data between a SIM device and an application executed in a trusted platform, wherein the data to be exchanged is secured from unauthorized access (Claim 1, 15, 23 of copending application publication).

Claim 2 recites The method of claim 1, wherein the exchanging of data include: exchanging an encryption key via a trusted path within a computer system; and exchanging data encrypted with the encryption key, via an untrusted path within the computer system (Claim 2 of copending application publication).

Claim 13 recites A system comprising: a processor; a memory having a protected section and an unprotected section; a SIM device; and a chipset to Exchange

data between the SIM device and an application executed in a trusted platform, wherein the data to be exchanged is secured from unauthorized access (Claims 11, 19, 23 of copending application publication).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

18. Applicant's argument on traversing nonstatutory obviousness type double patenting in view of claims 1, 2, 11, 15, 19 and 23 of copending Application No. 10/977,158 is acknowledged, it is not persuasive at this time.

First, the newly added claim limitations to independent claims 1, 2 and 13 of the current application are rejected under 35 USC § 112 first/second paragraphs as applied above.

Second, the limitations "trust port is mapped to a protected session..." and "protected section that is inaccessible to direct memory access..." in the current application and limitation "to generate a session key to encrypt data to be transmitted between the device and the application" in the co-pending application are obvious to a person with ordinary skill in the art in comparison with the current application. Although the conflicting claims are not identical, they are not patentably distinct from each other and encompass the same subject matter.

Therefore, nonstatutory obviousness type double patenting rejection is maintained.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

6 January 2008
AYS

THANHNGA TRUONG
PRIMARY EXAMINER